UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,660	05/01/2006	Richard Middleton Hicks	9664-0003	8461

73552 7590 05/26/2009

Stolowitz Ford Cowger LLP
621 SW Morrison St
Suite 600
Portland, OR 97205

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
05/26/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/577,660	**Applicant(s)** HICKS, RICHARD MIDDLETON	
	Examiner PAUL CALLAHAN	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20 and 22-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9-20 and 22-31* is/are rejected.

7)☒ Claim(s) *7and 8* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 May 2006* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *10-20-06*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-20 and 22-31 are pending and have been examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

3. The drawings are objected to because the labeling and numbering of the figures are hand-drawn and non-compliant. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required

corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 11-20 and 22-31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The preamble of claim 31 indicates that it is directed towards a software product. However, the claim does not positively recite any limitation that specifies the software as being embodied in a tangible, computer-readable storage medium. The Applicant's Specification does not specify what types of computer-readable media are contemplated for use with the invention. Therefore a reasonably broad construction of the claim language must include transmission media such as electromagnetic carrier waves. As such, the claim sets forth only functional descriptive language and is non-statutory since this does not fall into one of the classes of invention eligible for the grant of a US patent. Unless embodied in a computer-readable medium the software in and of itself cannot be considered as a computer component, and hence cannot effect a change of state of a processor to produce a useful or tangible result. From 2106.01: Computer-Related Nonstatutory Subject Matter: *Descriptive material can be* *characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions.*" The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) *"Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data. Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. *When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases.*

Claims 22-30 are dependent on claim 31 and do not cure its deficiency. Therefore they are rejected on the same basis as is claim 31.

As for claim 11, the preamble of the claim indicates that it is directed towards an apparatus. However, there are no positive recitations of any limitation in claim 11 or its dependent claims that are directed towards a hardware or firmware component. All of the claim limitations are directed towards method steps that are carried out in software, and as such the claims must be construed as directed towards a computer-program product. Additionally, the Applicant's Specification at paragraphs [0041]-[0042] state that the invention may be embodied entirely in software. Because claim 11 does not positively recite that the computer program is embodied in a tangible, computer readable storage medium, it is non-statutory for the same reasons set forth supra in the discussion of claim 31.

Claims 12-20 are dependent on claim 11 and do not cure its deficiency. Therefore they are rejected on the same basis as that claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1, 2, 6, 9-12, 16, 19, 20, 22, 26, and 29-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Cowie et al., US 2003/0023865 A1. Cowie discloses:

As for claim 1, a computer-implemented method for detection of items stored in a computer system such as computer code, data or information (Abstract, [0006]), the method comprising obtaining a signature by reading code comprising at least part of a program capable of introducing the items (fig. 5: element 18, [0015], [0034], [0048]), the code incorporating sufficient data to characterize the program adequately (fig. 5: element 18, [0034], [0048]), using the code as the signature (fig. 5: element 18, [0034], [0048]), comparing the signature with files stored on the computer system, and, if a match with the signature is found, providing an indication thereof ([0048], [0050], [0051]).

As for claim 2, a method according to claim 1 wherein the indication incorporates an identification of at least one of a) an item responsible for the match, b) the nature of the item, c) the item's location in the computer system, and d) the matching signature ([0048]).

As for claim 6, a method according to claim 1 wherein the step of comparing the signature with files is for each file preceded by checking the respective real file type by reading the start of the file and excluding files having prearranged initial byte sequences from comparing with the signature (fig. 6 element 32, [0049]: initial byte sequence is used to determine if file is a WIN32 PE file and if not, exclude it from further processing).

As for claim 9, a method according to claim 1 wherein files compared with the signature include self-extracting executable files and polymorphic files ([0050]).

As for claim 10, a method according to claim 1 wherein in respect of some prearranged files no indication as aforesaid is given despite their containing code which matches a signature ([0050]).

As for claims 11, 12, 16, 19, and 20, the claims are directed towards the apparatus carrying out the method of claims 1, 2, 6, 9, and 10. Claims 11, 12, 16, 19 and 20 recite substantially the same limitations as claims 1, 2, 6, 9, and 10 and are therefore rejected on the same basis as that claim.

As for claim 31, 22, 26, 29, and 30, the claims are directed towards a computer program product that directs a processor to carry out the method of claims 1, 2, 6, 9, and 10. Claims 31, 22, 26, 29 and 30 recite substantially the same limitations as claims 1, 2, 6, 9, and 10 and are therefore rejected on the same basis as that claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 3-5, 13-15, and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cowie et al., and Pierre Richer: SANS/GIAC Practical Assignment for GSEC Certification Version 1.4b: Steganalysis: Detecting hidden information with computer forensic analysis, SANS Institute 2003 (Submitted with the Applicant's IDS).

As for claim 3, Cowie et al. teach a method according to claim 1, but not explicitly wherein the items are steganographic items. However Richer does teach such a feature (page 6: Detecting Hidden Information With Various Resources: 1.) Guidance Software Inc. where comparisons of an original file MD5 hash is made with a MD5 hash of a suspect file in order to detect steganographically embedded data. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie. It would have been obvious to do so since this would extend the types of embedded malware detectable via the comparison step of Cowie.

Claim 13 represents the apparatus carrying out the method steps of claim 3. Claim 13 recites substantially the same limitation as claim 3 and is therefore rejected on the same basis as that claim.

Claim 23 represents the computer-program product that directs a processor to undertake the method steps of claim 3. Claim 23 recites substantially the same limitation as claim 3 and is therefore rejected on the same basis as that claim.

As for claim 4, Cowie teaches the method according to claim 1, but not explicitly wherein the code that is read is one of the following: a) a continuous sequence of program code; b) a continuous sequence of program code and beginning where its program begins, c) a continuous sequence of program code but not more than 5% and not less than 0.167% of its program's code; d) a program kernel; e) a .DDL or .ocx file; and f) code implementing both write to and read from a file. However Richer does teach such a feature (page 6: Detecting Hidden Information With Various Resources: 1.) Guidance Software Inc., where a continuous sequence of original file is read to form an MD5 hash, and then a comparison is made with a MD5 hash of a suspect file in order to detect embedded data. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie. It would have been obvious to do so since this would extend the types of files where embedded malware is detectable via the comparison step of Cowie.

Claim 14 represents the apparatus carrying out the method steps of claim 4. Claim 14 recites substantially the same limitation as claim 4 and is therefore rejected on the same basis as that claim.

Claim 24 represents the computer-program product that directs a processor to undertake the method steps of claim 4. Claim 24 recites substantially the same limitation as claim 4 and is therefore rejected on the same basis as that claim.

As for claim 5, Cowie teaches a method according to claim 1, but not explicitly asserted file type is ignored when comparing files with the signature. However Richer does teach such a feature (page 6: Detecting Hidden Information With Various Resources: 1.) Guidance Software Inc., where an original file is read in the process of forming an MD5 hash, and then a comparison is made with a MD5 hash of a suspect file in order to detect embedded data, all without reference to file types. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate this feature into the system of Cowie. It would have been obvious to do so since this would extend the types of files where embedded malware is detectable via the comparison step of Cowie.

Claim 15 represents the apparatus carrying out the method steps of claim 5. Claim 15 recites substantially the same limitation as claim 5 and is therefore rejected on the same basis as that claim.

Claim 25 represents the computer-program product that directs a processor to undertake the method steps of claim 5. Claim 25 recites substantially the same limitation as claim 5 and is therefore rejected on the same basis as that claim

Allowable Subject Matter

10. Claims 7 and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent documents teach methods of detection of embedded code utilizing hash comparison, where the methods are applicable to the Applicant's disclosure:

Angelo et al.	7,003,672
McGee et al.	6,694,434

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Paul Callahan/
Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437